Security incident report

Section 1: Identify the network protocol involved in the incident
In the incident described, several network protocols are involved in the process of connecting to the website and handling the attack. Here's a detailed breakdown of the network protocols used and the recommended security action to prevent future brute force attacks: 1. **HTTP (Hypertext Transfer Protocol)** - HTTP request to `yummyrecipesforme.com` for the web page. HTTP request to `greatrecipesforme.com` after the malware download and redirection.

Section 2: Document the incident
Incident Documentation **Incident Title:** Compromise of yumrecipesforme.com Due to Brute Force Attack and Malware Injection **Incident Date:** 7/29/2024 **Incident Description:** A former employee executed a brute force attack on the administrative account of yumrecipesforme.com, exploiting the default password to gain unauthorized access. Once inside, they modified the website's source code by embedding a JavaScript function that prompted visitors to download and execute a malicious file. This file redirected users to a fraudulent website, greatrecipesforme.com, which contained malware. Users reported slow performance and suspicious website behavior after running the

file.

Network Protocols Involved:

1. **HTTP (Hypertext Transfer Protocol):** Facilitated the initial web page request and the subsequent redirection to the malicious site. HTTPS may have been used but is not explicitly mentioned in the logs.

Incident Timeline:

1. **DNS Request:** Browser requests IP address for `yummyrecipesforme.com`.
2. **DNS Response:** IP address for `yummyrecipesforme.com` is provided.
3. **HTTP Request:** Browser requests web page from `yummyrecipesforme.com`.
4. **Malware Download:** Browser initiates download of a file from the compromised website.
5. **DNS Request:** After download, browser requests IP address for `greatrecipesforme.com`.
6. **DNS Response:** IP address for `greatrecipesforme.com` is provided.
7. **HTTP Request:** Browser requests web page from `greatrecipesforme.com`, containing malware.

Actions Taken:

1. A sandbox environment was created to analyze the malicious behavior.
2. Network protocol analyzer `tcpdump` was used to observe traffic and confirm redirection to the malicious site.
3. Incident was reported to senior analysts, confirming the compromise and identifying the presence of malware in the source code.

Section 3: Recommend one remediation for brute force attacks

Recommendations:

1. **Implement Strong Password Policies:** Enforce complex passwords and avoid defaults.
2. **Enable Account Lockout:** Prevent excessive login attempts.
3. **Use Multi-Factor Authentication (MFA):** Add an extra security layer for administrative accounts.
4. **Monitor and Alert:** Set up monitoring for suspicious activities.
5. **Deploy a Web Application Firewall (WAF):** Protect against various attack vectors.
6. **Regularly Update and Patch Systems:** Ensure all software is up-to-date.
7. **Conduct Security Audits:** Perform regular security assessments to identify and address vulnerabilities.